Kritische Infrastrukturen, Cybersicherheit, Datenschutz: die EU schlägt Pflöcke für digitale Standortpolitik ein

Bendiek, Annegret

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

Kritische Infrastrukturen, Cybersicherheit, Datenschutz

Die EU schlägt Pflöcke für digitale Standortpolitik ein

Annegret Bendiek

Die EU beabsichtigt, eine Meldepflicht für Cyberattacken auf kritische Infrastrukturen einzuführen. Zwar gibt es in Wirtschaft und Politik Widerstände gegen diesen Vorschlag, doch spricht einiges dafür, dass mit einer solchen Meldepflicht kritische Infrastrukturen präventiv geschützt werden können. Ausschlaggebend hierfür ist, dass die nationalen und europäischen Behörden die erlangten Informationen vertraulich behandeln und verarbeiten. Mit einem umfangreichen Maßnahmenkatalog setzt die EU Maßstäbe für eine europäische und internationale digitale Standortpolitik.

Oft wurde in den vergangenen Jahren auf die enormen Vorteile der Digitalisierung für das Wirtschaftswachstum hingewiesen. Die Europäische Kommission schätzt, dass Europa sein BIP um fast 500 Mrd. Euro jährlich (also um durchschnittlich 1000 Euro pro Kopf) steigern kann, sobald der digitale Binnenmarkt vollendet ist. Damit sich die hiermit verbundenen Technologien wie elektronische Zahlungen, Cloudcomputing oder Industrie 4.0 (etwa »Internet der Dinge« oder »Internet der Dienste«) durchsetzen können, muss dauerhaft Vertrauen bei den Bürgern geschaffen werden. Dazu hat die EU im Mai 2010 die Digitale Agenda verabschiedet. Mit ihren jüngsten Initiativen zu Cybersicherheit, Cloudcomputing, Datenschutz und elektronischer Identifizierung von Konsumenten setzt die EU wichtige Eckpfeiler für eine digitale Standortpolitik Europas. Die wachsende Regelungskompetenz der EU in diesem Bereich hat rechtliche, ökonomische und politische Auswirkungen auf die Mitgliedstaaten und enge Wirtschaftspartner wie die USA.

Die Digitalisierung von Infrastruktur, Wertschöpfungsketten und Lebenswelt eröffnet jedoch nicht nur Chancen, sondern birgt auch Risiken. Immer wieder lässt sich beobachten, wie anfällig das digitale Umfeld in den kritischen Infrastrukturen ist. Beim weltgrößten Ölkonzern Aramco (Saudi-Arabien) etwa wurden im August 2012 rund 30 000 Büro-PCs mit einer Schadsoftware infiziert. Im September desselben Jahres wurde die Deutsche Telekom Zielscheibe von Angriffen auf Domains ihrer Kunden. Hätten die Attacken »Erfolg« gehabt, wäre die Internetnutzung der Telekom-Kunden empfindlich gestört

Dr. Annegret Bendiek ist stellvertretende Leiterin der Forschungsgruppe EU-Außenbeziehungen

worden. Auch die Webseite der Sparkassen-Finanzgruppe wurde im Februar 2013 gehackt: Wer an diesem Tag »Sparkasse.de« ansteuerte, lief Gefahr, dass sein Rechner von einer dort platzierten Schadsoftware beeinträchtigt wurde.

Schutz kritischer Infrastruktur

Nach jüngsten Untersuchungen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) nehmen Sicherheitsvorfälle im Cyberraum mit alarmierender Geschwindigkeit zu. Die Angreifer könnten sogar die Bereitstellung grundlegender Dienste wie Wasserversorgung, Gesundheitsfürsorge, Strom oder Mobilfunk stören oder sabotieren. Daher legt die EU besonderes Augenmerk auf die kritischen Infrastrukturen, die weitestgehend in privater Hand sind. Dabei fasst sie den Begriff sehr weit (siehe Tabelle), da sie ihre Priorität auf einen funktionierenden Binnenmarkt legt und nicht allein auf die Selbstregulierung privater Akteure. Der Schutz kritischer Infrastrukturen ist Voraussetzung für die Vollendung des digitalen Binnenmarkts, der wiederum notwendig für das dauerhaft reibungslose Funktionieren des Binnenmarkts sein wird.

Die EU-Kommission will mit ihrer Digitalen Agenda einen digitalen Binnenmarkt für Inhalte und Dienste schaffen, der die Vorteile des digitalen Zeitalters zur Geltung bringen soll. Im grenzüberschreitenden Waren-, Dienstleistungs- und Personenverkehr spielen digitale Informationssysteme, allen voran das Internet, eine wesentliche Rolle, denn diese Kommunikationsmittel sind in allen Mitgliedstaaten miteinander vernetzt. Eine schwere Störung dieser Systeme in einem Mitgliedstaat kann auch andere Mitgliedstaaten und die EU insgesamt in Mitleidenschaft ziehen. Darum handelt es sich bei der Digitalen Agenda um eine europäische Aufgabe. Denn wenn sich Sicherheitsvorfälle häufen und es keinen wirksamen Schutz dagegen gibt, dürfte die Bereitschaft abnehmen, Netze und Informationssysteme zu nutzen. Dies hätte negative wirtschaftliche Konsequenzen für den Binnenmarkt. Laut Eurobarometer glauben 38 Prozent der Internetnutzer in der EU, dass Online-Zahlungen nicht sicher sind.

EU-Strategie zur Cybersicherheit

Sicherheit im Cyberraum lässt sich nicht erreichen, wenn sie nur als Aufgabe einiger weniger IT-Spezialisten oder als technische Herausforderung einzelner Unternehmen verstanden wird. Cybersicherheit erfordert konzertiertes Handeln von Wirtschaft, Politik und Gesellschaft auf allen Ebenen der Politik. Diesem Multistakeholder-Ansatz folgen auch die erste Cybersicherheitsstrategie der EU, die im Februar 2013 von der Europäischen Kommission und dem Europäischen Auswärtigen Dienst präsentiert wurde, sowie ein EU-Richtlinienvorschlag für Netz- und Informationssicherheit (NIS). Zusammen mit dem Anfang Januar 2013 eröffneten Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) sollen diese Initiativen den Weg ebnen, im europäischen Verbund gegen Cybergefahren vorzugehen. Das EC3 ist Teil des Europäischen Polizeiamts (Europol) und dient als zentrale Anlaufstelle für die Bekämpfung der Cyberkriminalität in der EU.

Diese Strategie hat zum Ziel, Sicherheitsstandards von Informations- und Kommunikationstechnologien zu gewährleisten und gleichzeitig die Grundrechte und Grundwerte der EU zu wahren. Sie sieht vor, die Öffentlichkeit für das Sicherheitsproblem zu sensibilisieren, einen Binnenmarkt für Cybersicherheitsprodukte und -dienste aufzubauen sowie Investitionen in Forschung und Entwicklung zu fördern. Ergänzt werden sollen diese Maßnahmen um eine verstärkte Cyberkriminalitätsbekämpfung und eine internationale Cybersicherheitspolitik.

In ihrem Richtlinienvorschlag hebt die Kommission die besondere Rolle privatwirtschaftlicher Unternehmen hervor. Nicht nur die Mitgliedstaaten, sondern auch die Betreiber kritischer Infrastrukturen müssen

Kritische Infrastrukturen aus Sicht der EU
Richtlinienvorschlag für Netz- und Informationssicherheit (NIS)

Nach Artikel 3 Absatz 8 Buchstabe a
Marktteilnehmer
Plattformen des elektronischen Geschäftsverkehrs, Internet-Zahlungs-Gateways, Soziale Netze, Suchmaschinen, Cloudcomputing-Dienste, Application Stores
Nach Artikel 3 Absatz 8 Buchstabe b
Energie
Strom- und Gasversorger, Verteilernetzbetreiber und Endkundenlieferanten im Strom- und/oder Gassektor, Erdgas-Fernleitungsnetzbetreiber, Erdgasspeicher- und LNG-Anlagenbetreiber, Übertragungsnetzbetreiber (Strom), Erdöl- und Gasmarktteilnehmer, Betreiber von Erdöl- und Erdgas-Produktions-, Raffinations- und Behandlungsanlagen
Verkehr
Luftfahrtunternehmen (Luftfrachtverkehr und Personenbeförderung), Beförderungsunternehmen des Seeverkehrs (Personen- und Güterbeförderung in der See- und Küstenschifffahrt), Eisenbahnen (Infrastrukturbetreiber, integrierte Unternehmen und Eisenbahnunternehmen), Flughäfen, Häfen, Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, unterstützende Logistikdienste: a) Lagerhaltung und Lagerung b) Frachtumschlagsleistungen und c) andere unterstützende Verkehrsleistungen
Bankwesen
Kreditinstitute nach Artikel 4 Absatz 1 der Richtlinie 2006/48/EG
Finanzmarktinfrastrukturen
Börsen und Clearingstellen mit zentraler Gegenpartei
Gesundheitswesen
Einrichtungen der medizinischen Versorgung (einschließlich Krankenhäusern und Privatkliniken) sowie andere Einrichtungen der Gesundheitsfürsorge

demnach ihren Teil zum Schutz der weltweiten digitalen Infrastruktur beitragen. Die Unternehmen sollen dafür sorgen, dass ihre Produkte und Dienstleistungen stets aktuellen Sicherheitsstandards genügen und so gut wie möglich gegen Angriffe gewappnet sind.

Wirtschaftsexperten bewerten den EU-Ansatz als wichtigen und richtigen europäischen Schritt. Für seine Umsetzung aber fordern Lobbyorganisationen wie der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) eine klare Methodologie für die einzelnen Branchen. Die EU-Initiative wird international und innereuropäisch unterstützt, weil sie auf den Erfahrungen führender europäischer Nationen in der Cybersicherheit wie Deutschland, Frankreich, Großbritannien, Niederlande und Schweden aufbaut. Während die Nato-Strategie auf Cyberverteidigung und die US-Strategie auf Abschreckung (Cyber Deterrence) setzen, legt die EU-Strategie ihre Schwerpunkte auf den Schutz kritischer Infrastrukturen und die Cyberkriminalitätsbekämpfung.

Maßvolle und verbindliche Regulierung

Mehr als ein Drittel aller Entscheidungsträger aus Wirtschaft und Politik ist überzeugt, dass Europa beim Thema Datensicherheit und -schutz aktiver werden sollte. Im Gegensatz zur US-amerikanischen Debatte meinen in Deutschland rund 57% der befragten Wirtschaftsvertreter und 77% der Befragten im Bereich Politik, dass nicht nur private Unternehmen, sondern auch staatliche Stellen dafür zuständig sein

sollten, die Funktionsfähigkeit der Kommunikations- und Datenübertragungsnetze zu sichern. Um diesen Erwartungen gerecht zu werden, erscheint eine maßvolle Regulierung kritischer Infrastrukturen sinnvoll, die aus Sicht der EU allerdings auch verbindlich sein soll. Nach EU-Strategie und -Richtlinienvorschlag soll die IT-Sicherheit in Europa auf vierfache Weise verbessert werden.

Meldepflicht

Betreiber kritischer Infrastrukturen haben eine besondere gesamtgesellschaftliche Verantwortung, weil eine Beeinträchtigung oder gar ein Ausfall dieser Infrastrukturen gravierende Folgen zeitigen können. Daher sollen die Betreiber darauf verpflichtet werden, den Schutz der von ihnen eingesetzten Informationstechnik zu verbessern und ihre Kommunikation mit dem Staat zu intensivieren. Die Meldepflicht für IT-Sicherheitsvorfälle, wie sie Innenminister Hans-Peter Friedrich in seinem Entwurf für ein deutsches IT-Sicherheitgesetz propagiert, ist in Wirtschaft und Politik stark umstritten. Während der Bundesverband der Industrie (BDI) sie ablehnt, sprechen Sicherheitsbehörden sich dafür aus. Eine Meldepflicht soll demnach präventiven Schutz der IT kritischer Infrastrukturen sicherstellen. Die ENISA auf europäischer und das Bundesamt für Sicherheitstechnik (BSI) auf nationaler Ebene diskutieren derzeit, wie die vertrauliche Behandlung der erlangten Informationen gewährleistet werden kann. Unternehmensvertreter fordern, dass der Staat die Daten anonymisiert, damit betroffene Firmen nicht diskreditiert werden. Verschärfungen wie etwa eine Meldepflicht für jede rechtzeitig erkannte Sicherheitslücke jedoch führen nach Ansicht der Unternehmen zu weit.

Die Telekommunikations- und Telemediendienstanbieter spielen eine Schlüsselrolle für die Sicherheit des Cyberraums. Sie sollen nachdrücklicher als bisher in die Verantwortung genommen werden. Um die wachsenden Herausforderungen bei der Kriminalitätsbekämpfung zu meistern, sollen Behörden, Politik, Wirtschaft und Wissenschaft eng zusammenarbeiten. Die Organe, Einrichtungen und sonstigen Stellen der EU haben ihr eigenes IT-Notfallteam (Computer Emergency Response Team, CERT) geschaffen, das »CERT-EU«. Mit ihrem Vorhaben, nationale CERTs einzuführen, setzt die EU das richtige Signal. Deutschland hat schon 2001 beim BSI das »CERT Bund« eingerichtet. Andere EU-Staaten haben erst in den letzten Jahren nationale CERT-Strukturen aufgebaut.

Mehr Problembewusstsein (Awareness)

Die Bevölkerung in der gesamten EU muss über die Gefahren im Cyberspace informiert und dafür sensibilisiert werden. In Deutschland wurde 2012 auf Initiative des BSI die »Allianz für Cybersicherheit« gegründet, um die Cybersicherheit hierzulande zu verbessern. Die Erfahrungen daraus können auch für die EU wegweisend sein. Doch auch die Bürger selbst sind aufgefordert, für mehr Sicherheit zu sorgen. Ein entscheidendes Schlagwort dabei lautet »Bring your own device« (BYOD). Das bedeutet, dass elektronische Geräte entweder nur privat oder nur geschäftlich genutzt werden sollen. Eines lässt sich nicht durch Vorschriften regulieren – der Faktor Mensch.

Die EU setzt einen rechtlichen Rahmen für mehr Kooperation und freiwillige Initiativen in der Cybersicherheit. Das Maß der Selbstregulierung bleibt mit dem Richtlinienvorschlag aber so hoch wie möglich und die gesetzlichen Vorgaben sollten für alle Beteiligten einen Mehrwert bringen. Eine zentralisierte europäische Überregulierung dagegen würde die Entwicklung innovativer technologischer Lösungen verlangsamen und Industrie und Regierung in ihren Möglichkeiten beschneiden, angemessen auf die dynamische Bedrohungslage zu reagieren. Hauptinstrument für eine verbindliche und maßvolle Regulierung auf EU-Ebene sind Public-Private Partnerships (PPP).

Neue Rolle für die ENISA

Die europäische Schnittstelle für die PPP in der Cybersicherheit ist die ENISA. Ihr Mandat ist jüngst bis 2017 verlängert worden. Zwar soll sie nicht so stark operativ tätig sein wie etwa das deutsche BSI beim Schutz der Bundesverwaltung. Die ENISA berät die Institutionen der EU sowie der Mitgliedstaaten, hat also zunächst eher ein beratendes Mandat. Allerdings wächst der operative Teil ihrer Arbeit. Für eine schnelle und effektive Reaktion auf Vorfälle im Internet ist es entscheidend, Abläufe und Informationsflüsse zu kennen. Das betrifft insbesondere Mitgliedstaaten, die in der Netz- und Informationssicherheit schlechter dastehen. Kontinuierliche Zusammenarbeit zwischen öffentlichen und privaten Akteuren ist ebenfalls wichtig, vor allem weil PPPs in den einzelnen Ländern Europas sehr unterschiedliche Formen annehmen können. Die ENISA bündelt Wissen über die kollektive Fähigkeit der EU in der Cyberabwehr.

Übungen zur Cybersicherheit

Ende 2012 nahmen mehr als 500 europäische Fachleute aus 29 EU-/EFTA-Staaten an »Cyber Europe 2012« teil, der zweiten europaweiten Übung zur Cybersicherheit. Sie sollte helfen, kritische Infrastrukturen auf nationaler und europäischer Ebene robuster zu machen. Die Übung war ein Meilenstein im Bemühen, die Zusammenarbeit, Abwehrbereitschaft und Reaktionsfähigkeit im Fall von Cyber-Sicherheitskrisen in Europa zu stärken. Auf Basis der in den vergangenen Jahren ausgeweiteten Regulierungskompetenz der EU wurden Gegenstand, Umfang und Komplexität von Cyber Europe 2012 ausgedehnt. Unter anderem sollten Lücken beim Umgang mit weitreichenden Netzstörungen in Europa ermittelt werden.

Darüber hinaus veranstalteten EU und USA im November 2011 eine gemeinsame Planübung (»Cyber Atlantic 2011«). Weitere Übungen, auch auf internationaler Ebene, sind für die nächsten Jahre vorgesehen. Die ENISA entwickelt sich derzeit zum Ansprechpartner für internationale Übungen zur Cybersicherheit.

Provider und Cloudcomputing

Im Zuge der Digitalisierung von Infrastrukturen lassen sich fünf unterschiedliche »intelligente Netze« identifizieren, in denen Informations- und Kommunikationstechnologie (IKT) zu enormen Effizienzsteigerungen führt: e-Government, e-Mobility, e-Energy, e-Health und e-Learning. Neben den genannten Maßnahmen zur Verbesserung der IT-Sicherheit kritischer Infrastrukturen im Allgemeinen enthält deshalb der aktuelle Richtlinienvorschlag der EU Inhalte speziell für Anbieter von Diensten der Informationsgesellschaft. Auf diese Dienste stützen sich nachgelagerte Dienste oder Online-Tätigkeiten wie Plattformen des elektronischen Geschäftsverkehrs, Internet-Zahlungs-Gateways, Soziale Netze, Suchmaschinen, Cloudcomputing-Dienste und Application Stores (siehe Tabelle).

Ausweitung der IKT

Bisher müssen Unternehmen, die öffentliche Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste bereitstellen, angemessene Schutzmaßnahmen ergreifen. Außerdem unterliegen sie einer Meldepflicht für den Fall von Sicherheitsverletzungen und Integritätsverlust.

Die Nutzer als schwächstes Glied in der Kette sollen in die Lage versetzt werden, Störungen, die von ihren Systemen ausgehen, zu erkennen und möglichst auch zu beseitigen. Zu diesem Zweck sollen Provider ihre Nutzer über bekannt gewordene Störungen unterrichten und Hinweise liefern, wie diese sich entfernen lassen. Weil sich Schadsoftware schon über das bloße Ansurfen von Webseiten (sog. Drive by Exploit) verbreiten kann, sollen auch die professionellen Webseitenanbieter mehr für die Sicherheit des Gesamtsystems tun. Deswegen sollen den Anbietern Vorgaben

gemacht werden, die Maßnahmen zum Schutz vor unerlaubten Zugriffen vorsehen. Die Wertschöpfung des europäischen Sektors für Informations- und Kommunikationstechnologien beläuft sich auf rund 600 Mrd. Euro. Dem Druck zur Anpassung an wirtschaftliche Notwendigkeiten kann sich kaum jemand entziehen.

EU-Cloudcomputing

Die EU strebt auch ein EU-weites Cloudcomputing-System an, um die derzeitigen unterschiedlichen gesetzlichen Bestimmungen auf nationaler Ebene zu vereinheitlichen. Damit will sie mehr Vertrauen in Datensicherheit und Verbraucherschutz schaffen. Bei allen Verwaltungsvorgängen bis hin zu Analysen, Vorlagen und Verträgen sind Dateien im Spiel – und fast immer in der Zusammenarbeit mit Partnern außerhalb der EU. Mitarbeiter von Unternehmen beispielsweise sind darauf angewiesen, jederzeit ortsunabhängigen Zugriff auf teilweise hochvertrauliche Daten erhalten zu können. Doch Dateien, die auf Cloud-Plattformen wie Dropbox, Google Drive oder Skydrive abgelegt werden, können sich als ernstes Sicherheitsrisiko herausstellen. Gefahren lauern etwa in außereuropäischen Servern und in Allgemeinen Geschäftsbedingungen (AGBs), die teilweise weitreichende Zugriffsrechte auf den Inhalt einschließen; und auch Einbruchsszenarien wie zuletzt bei Dropbox sind zu befürchten.

Aus diesen Gründen hat die Kommission Ende September 2012 eine Strategie zur »Freisetzung des Cloud-Computing-Potenzials in Europa« vorgelegt. Im Zuge der Strategie sollen die technischen Normen harmonisiert werden. Zudem sollen EU-weite Zertifizierungsprogramme für vertrauenswürdige Cloud-Anbieter unterstützt sowie sichere und faire Muster-Vertragsbedingungen erarbeitet werden. Die Kommission will eine Europäische Cloud-Partnerschaft mit den Mitgliedstaaten und der Branche etablieren, um die Marktmacht des öffentlichen Sektors besser nutzbar zu machen. Auf diese Weise sollen auch europäische Cloud-Anbieter mehr Chancen erhalten, eine wettbewerbsfähige Größe zu erreichen. Damit ließen sich elektronische Behördendienste auf die Dauer verbilligen und verbessern. Das Ziel lautet, bis 2020 rund 2,5 Mio. neue IT-Arbeitsplätze in Europa zu schaffen und das BIP der EU um 160 Mrd. Euro jährlich zu steigern.

Datenschutz

Der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (EP) ist den Risiken des Cloudcomputing bereits 2012 auf den Grund gegangen und wollte wissen, ob mit dessen Zunahme auch die Cyberkriminalität ansteige und ob gehandelt werden müsse. Dabei kam heraus, dass ein Sicherheitsrisiko vorrangig im Verlust über die Kontrolle von Daten besteht, wenn diese beispielsweise auf den Servern von US-Anbietern liegen. US-Behörden können sich heimlich Zugriff auf die Daten europäischer Nutzer von Cloud-Anbietern wie Google, Facebook oder Dropbox verschaffen. Das wurde im vom EP in Auftrag gegebenen Gutachten des Centre d'Etudes Sur Les Conflits und des Centre for European Policy Studies festgestellt. Juristen der Universität Amsterdam haben ebenfalls im November 2012 darauf hingewiesen, dass der Patriot Act den US-Geheimdiensten umfangreiche Zugriffsrechte auf Kommunikations- und Nutzerdaten einräumt. Auf der Rechtsgrundlage der Antiterrorgesetze Patriot Act und Foreign Intelligence Surveillance Amendment Act (FISAA) von 2008, der bis 2017 verlängert wurde, können US-Ermittler bei einem Gericht einen geheimen Beschluss beantragen und ausländische Nutzer überwachen. Demnach müssen nicht nur amerikanische Cloud-Anbieter wie Google oder Amazon die Daten ihrer Kunden auf Anfrage (optional mit der Verpflichtung zur Geheimhaltung) herausgeben – ungeachtet dessen, ob die Daten sich auf Servern in Europa oder den USA befinden. Es können

auch europäische Firmen betroffen sein, die in den USA geschäftlich tätig sind.

Rechtssicherheit beim Cloudcomputing sollte daher Priorität genießen. Zudem sind Verhandlungen mit den USA nötig, um das Menschenrecht auf Privatsphäre für europäische Staatsbürger zu garantieren. Denn wenn Cloud-Daten von der EU in die USA überführt werden, unterliegen diese dem Zugriff der US-Behörden, wie die Aussagen des ehemaligen US-Geheimdienstlers Edward Snowden Anfang Juni 2013 offenbar bestätigen. Um Daten auf Vorrat zu speichern, zu analysieren und zu verwerten, errichtet der US-Geheimdienst NSA derzeit ein gigantisches Rechenzentrum in Utah. Welchen Stellenwert die Big-Data-Analyse in den US-Geheimdiensten hat, zeigen die Enthüllungen in der sogenannten Prism-Affäre. »Prisma« heißt das Überwachungsprogramm der NSA, in Anspielung auf die Reflexion von Licht in Glasfaserkabeln. Diese Kabel sind das Rückgrat des weltweiten Internetverkehrs.

Artikel 43a

Vor diesem Hintergrund diskutiert das Europäische Parlament zurzeit einen Zusatz in der EU-Datenschutzverordnung, der die Weitergabe europäischer Daten an die US-Behörden untersagt. Die noch gültige Datenschutzrichtlinie aus dem Jahr 1995 verbietet es, personenbezogene Daten aus EU-Mitgliedstaaten in Länder zu übertragen, die nicht über einen dem EG-Recht vergleichbaren Datenschutz verfügen. Dazu gehören auch die USA. Mit der im Jahr 2000 zwischen EU und USA geschlossenen Datenschutzvereinbarung »Safe Harbour« jedoch konnten sich US-Unternehmen auf die »Grundsätze des sicheren Hafens« verpflichten lassen, um Daten aus Europa in den USA weiterzuverarbeiten. Die EU-Datenschutzrichtlinie sieht vor, dass die Verarbeitung sensibler personenbezogener Daten in der Regel nicht gestattet ist und nur in eng definierten Grenzen zugelassen wird. Das EU-Recht erlaubt, dass Polizei und Justiz bei Strafsachen in einem gesetzlich geregelten Verfahren auf bestimmte Daten zugreifen dürfen.

In den neuen Entwurf zur EU-Datenschutzverordnung fügte das Europäische Parlament den Artikel 43a wieder ein, den die Kommission zuvor nach starkem Druck der US-Regierung gestrichen hatte. Artikel 43a besagt, dass Unternehmen sensible Daten von EU-Bürgern nur noch dann ausländischen Sicherheitsbehörden übermitteln dürfen, wenn dies durch ein Rechtshilfeabkommen gedeckt wird. Solange sich die USA und die EU also nicht auf Regeln für den Datenaustausch einigen, müssen Unternehmen der US-Regierung die Herausgabe verweigern. Solche Rechtsunsicherheit bringt Firmen wie Facebook und andere in Schwierigkeiten. Die von der Überwachung betroffenen Internet-Unternehmen Google, Facebook und Microsoft haben daher in offenen Briefen die US-Regierung um Erlaubnis gebeten, alle Anfragen der Geheimdienste nach Nutzerdaten öffentlich zu machen.

Bis Ende 2013 wollen die Justizminister der Mitgliedstaaten und das Europäische Parlament einen endgültigen Entwurf vorlegen, der 2014 verabschiedet und 2016 in Kraft treten könnte. Ein weiterer strittiger Punkt ist das sogenannte Recht auf Vergessen, also weitgehende Löschrechte für Internetnutzer, wenn es um ihre Daten geht.

Schlussfolgerungen für die Europapolitik

Die Digitalisierung von Infrastrukturen, Wertschöpfungsketten und Lebenswelten bringt neue wirtschaftliche Potentiale für Europas Binnenmarkt. Diese lassen sich aber nur auf der Grundlage von Datenerhebung und -analyse ausschöpfen. In der aktuellen Europapolitik scheint dieser Zusammenhang nicht immer präsent zu sein. So ist es kaum vorstellbar, dass die Energiewende ohne die mit intelligenten Stromnetzen (Smart Grids) verbundene Datennutzung zu schaffen ist. Diese Ent-

wicklung greift die EU mit der dargelegten Digitalen Agenda auf.

Datennutzung ist unverzichtbar für Innovationen und die Bewältigung gesellschaftlicher Herausforderungen. Daher ist es eine politische Aufgabe, Vertrauen in diese Technologien zu erzeugen. Derzeit gibt es keinen umfassenden grenz- und sektorenübergreifenden EU-Rahmen für sichere, vertrauenswürdige und einfach zu nutzende Transaktionen, der elektronische Identifizierung, Authentifizierung und Signaturen einschließt. Darum muss es das Ziel sein, die bestehenden Rechtsvorschriften zu erweitern und die gegenseitige Anerkennung notifizierter elektronischer Identifizierungssysteme und anderer wichtiger elektronischer Vertrauensdienste auf EU-Ebene zu regeln. Der vorgeschlagene Rechtsrahmen, eine »Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt«, soll sichere und nahtlose elektronische Transaktionen zwischen Unternehmen, Bürgern und öffentlichen Verwaltungen ermöglichen. Auf diese Weise soll er die Effektivität öffentlicher und privater Online-Dienstleistungen, des elektronischen Geschäftsverkehrs und des elektronischen Handels in der EU erhöhen. Daher wäre es gewiss empfehlenswert, die Verordnung zu verabschieden.

Auch wenn die Meldepflicht für Betreiber kritischer Infrastrukturen in Europa der richtige Weg ist, sollte eine Überregulierung in Datenverarbeitung und Datenschutz vermieden werden. Sie ginge zu Lasten einer zügigen Entwicklung innovativer technologischer Lösungen. Überdies würde sie Industrie und Regierung womöglich dabei behindern, selbst wirksam gegen sich wandelnde Bedrohungen vorzugehen.

Der aktuelle Entwurf zur Datenschutzverordnung ist insofern kritisch zu sehen, als er viel zu sehr auf die Regulierung sozialer Medien ausgerichtet ist, aber das Potential der Datennutzung vernachlässigt, das ein wichtiger Wettbewerbsfaktor für die Wirtschaft ist. Gleichwohl sind alle Maßnahmen der Datenschutzverordnung zu begrüßen, wie Alex Pentland vom Massachusetts Institute of Technology (MIT) schon 2009 beim Weltwirtschaftsforum in Davos gefordert hat. Pentland hat dabei den alten englischen Rechtsbegriff der »Eigentümerschaft« als Referenz verwendet, der das »Recht des Besitzes«, das »Recht des Gebrauchs« und auch das »Verfügungsrecht« umfasst.

Beim Aufbau eines digitalen Binnenmarktes steht die EU vor der großen Aufgabe, bei der Datennutzung eine Brücke zwischen Innovation und Zukunftsherausforderungen einerseits sowie Sicherheit und Datenschutz andererseits zu schlagen. Cybersicherheit kann nur gewährleistet werden, wenn sie auf den in der Charta der EU garantierten Grundrechten und Grundfreiheiten und auf den Grundwerten der EU basiert. Die Rechte des Einzelnen können ihrerseits nur geschützt werden, wenn Netze und Systeme sicher sind. Vertrauen ist Voraussetzung dafür, dass Innovationen angenommen werden.

Mit dem vorgestellten Maßnahmenpaket schlägt Europa Pflöcke für eine digitale Standortpolitik ein, für einen der sichersten digitalen und zugleich freiheitlich bestimmten regionalen Standorte kritischer Infrastrukturen weltweit. Die deutsche Europapolitik wäre gut beraten, Europas digitale Standortpolitik als politische Priorität in der nächsten Legislaturperiode voranzutreiben.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6364